GreenPoint Legal

SSL SECURITY: HEARTBLEED AND HEADACHE

In March of 2012, version 1.0.1 of OpenSSL — the open-source Internet-encryption software utilizing Secure Socket Layering — was released, and by 2014, that version, commonly known as the "Heartbeat Extension," was in use by two-thirds of all web servers. The only problem was that OpenSSL developers had missed a string of flawed codes, and that "bug" — permitting serious security vulnerability — changed "Heartbeat" to "Heartbleed." Now, new OpenSSL flaws have been discovered, and experts debate whether they pose a serious compromise of Internet security.

How Bad Was Heartbleed?

Simply put, the Heartbleed bug allowed attackers to obtain everything from user names and passwords to the "keys" used to encrypt and decrypt data otherwise presumed to be secure. The threat was so severe and widespread that the Federal Financial Institutions Examination Council (FFIEC) instructed U.S. financial institutions to "incorporate patches on systems and services, applications, and appliances using OpenSSL and upgrade systems as soon as possible to address the vulnerability" (FFIEC press release, April 10, 2014).

Notwithstanding the urgency of the OpenSSL crisis, tests conducted on the websites of several of the largest banks found all of them to be free of the vulnerability, and eight of the institutions issued statements that they do not rely on OpenSSL software for their customer-facing exchanges. Nevertheless, critical servers from the Canadian Tax Authority to various UK organizations were, in fact, attacked via Heartbleed holes, thus prompting OpenSSL users to heed the security advisory issued by OpenSSL.

Old Flaws Discovered

In the course of installing patches to remedy Heartbleed and undertaking other Internet security reviews, even older code flaws — some going back to 1998 — were discovered in the software. The good news, however, is that the latest-discovered flaws do not pose anywhere near the security compromise that Heartbleed did. Dubbed "man-in-the-middle" flaws, the worst one would require that both the client and server be running compromised versions of OpenSSL and that the malicious hacker be positioned in the middle at just the right moment. Since none of the most commonly used browsers, such as Internet Explorer, Firefox and Chrome, employ OpenSSL for encryption, web browser use is not deemed to be particularly vulnerable to the flaw.

The Next Steps

The organization that developed OpenSSL consists of only 11 developers — 10 of whom are volunteers — and one full-time staff member, the lead developer. The entire budget for the OpenSSL Project is less than $1 million per year garnered from donations. To address these shortcomings, the United States Department of Homeland Security, Microsoft and Google have teamed up to form the Core Infrastructure Initiative to properly fund Open SSL and other critical software elements used throughout the Internet.

CONTACT US!

DAVID T. KINNEAR
O: 212.913.0500 x565
M: 917.886.3222
E: DAVID.KINNEAR@GREENPOINTGLOBAL.COM

WILLIAM H. ANDERSON, ESQ
O: 212.913.0500 x586
M: 914.672.4975
E: WILLIAM.ANDERSON@GREENPOINTGLOBAL.COM

PETER K. OVERZAT, ESQ
O: 212.913.0500 x557
M: 917.807.1321
E: PETER.OVERZAT@GREENPOINTGLOBAL.COM

WWW.GREENPOINTLEGAL.COM